

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/751,366	12/29/2000	Stella Chan	342818008US	8258
25096	7590	08/16/2004	EXAMINER	
PERKINS COIE LLP PATENT-SEA P.O. BOX 1247 SEATTLE, WA 98111-1247			STARKS, WILBERT L	
			ART UNIT	PAPER NUMBER
			2121	

DATE MAILED: 08/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/751,366	CHAN ET AL.	
	Examiner	Art Unit	
	Wilbert L. Starks, Jr.	2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 21 April 2004.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-80 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 1-80 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a))

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .

5) Notice of Informal Patent Application (PTO-152)

6) Other: ____ .

DETAILED ACTION

Claim Rejections - 35 U.S.C. § 101

1. 35 U.S.C. §101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

the invention as disclosed in claims 1-80 is directed to non-statutory subject matter.

2. Regardless of whether any of the claims are in the technological arts, none of them is limited to practical applications in the technological arts. Examiner finds that *In re Warmerdam*, 33 F.3d 1354, 31 USPQ2d 1754 (Fed. Cir. 1994) controls the 35 U.S.C. §101 issues on that point for reasons made clear by the Federal Circuit in *AT&T Corp. v. Excel Communications, Inc.*, 50 USPQ2d 1447 (Fed. Cir. 1999). Specifically, the Federal Circuit held that the act of:

...[T]aking several abstract ideas and manipulating them together adds nothing to the basic equation. *AT&T v. Excel* at 1453 quoting *In re Warmerdam*, 33 F.3d 1354, 1360 (Fed. Cir. 1994).

Examiner finds that Applicant's "information identifying ... users that are members of the group" and "information identifying ... items that are members of the group" references are just such abstract ideas.

3. Examiner bases his position upon guidance provided by the Federal Circuit in *In re Warmerdam*, as interpreted by *AT&T v. Excel*. This set of precedents is within the

same line of cases as the *Alappat-State Street Bank* decisions and is in complete agreement with those decisions. *Warmerdam* is consistent with *State Street's* holding that:

Today we hold that the transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation because it produces 'a useful, concrete and tangible result' – a final share price momentarily fixed for recording purposes and even accepted and relied upon by regulatory authorities and in subsequent trades. (emphasis added) *State Street Bank* at 1601.

4. True enough, that case later eliminated the "business method exception" in order to show that business methods were not *per se* nonstatutory, but the court clearly *did not* go so far as to make business methods *per se statutory*. A plain reading of the excerpt above shows that the Court was *very specific* in its definition of the new *practical application*. It would have been much easier for the court to say that "business methods were *per se statutory*" than it was to define the practical application in the case as "...the transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price..."

5. The court was being very specific.

6. Additionally, the court was also careful to specify that the "useful, concrete and tangible result" it found was "a final share price momentarily fixed for recording purposes and even accepted and relied upon by regulatory authorities and in subsequent trades." (i.e. the trading activity is the further practical use of the real world monetary data beyond the transformation in the computer – i.e., "post-processing activity".)

Art Unit: 2121

7. Applicant cites no such specific results to define a useful, concrete and tangible result. Neither does Applicant specify the associated practical application with the kind of specificity the Federal Circuit used.

8. Furthermore, in the case *In re Warmerdam*, the Federal Circuit held that:

...[T]he dispositive issue for assessing compliance with Section 101 in this case is whether the claim is for a process that goes beyond simply manipulating 'abstract ideas' or 'natural phenomena' ... As the Supreme Court has made clear, '[a]n idea of itself is not patentable, ... taking several abstract ideas and manipulating them together adds nothing to the basic equation. *In re Warmerdam* 31 USPQ2d at 1759 (emphasis added).

9. Since the Federal Circuit held in *Warmerdam* that this is the “dispositive issue” when it judged the usefulness, concreteness, and tangibility of the claim limitations in that case, Examiner in the present case views this holding as the dispositive issue for determining whether a claim is “useful, concrete, and tangible” in similar cases. Accordingly, the Examiner finds that Applicant manipulated a set of abstract “information identifying … users that are members of the group” and “information identifying … items that are members of the group” to solve purely algorithmic problems in the abstract.

10. Since the claims are not limited to exclude such abstractions, the broadest reasonable interpretation of the claim limitations includes such abstractions. Therefore, the claims are impermissibly abstract under 35 U.S.C. §101 doctrine.

11. Since *Warmerdam* is within the *Alappat-State Street Bank* line of cases, it takes the same view of “useful, concrete, and tangible” the Federal Circuit applied in *State Street Bank*. Therefore, under *State Street Bank*, this could not be a “useful, concrete and tangible result”. There is only manipulation of abstract ideas.

12. The Federal Circuit validated the use of *Warmerdam* in its more recent *AT&T Corp. v. Excel Communications, Inc.* decision. The Court reminded us that:

Finally, the decision in *In re Warmerdam*, 33 F.3d 1354, 31 USPQ2d 1754 (Fed. Cir. 1994) is not to the contrary. *** The court found that the claimed process did nothing more than manipulate basic mathematical constructs and concluded that 'taking several abstract ideas and manipulating them together adds nothing to the basic equation'; hence, the court held that the claims were properly rejected under §101 ... Whether one agrees with the court's conclusion on the facts, the holding of the case is a straightforward application of the basic principle that mere laws

Art Unit: 2121

of nature, natural phenomena, and abstract ideas are not within the categories of inventions or discoveries that may be patented under §101.
(emphasis added) AT&T Corp. v. Excel Communications, Inc., 50 USPQ2d 1447, 1453 (Fed. Cir. 1999).

13. Remember that in *In re Warmerdam*, the Court said that this was the dispositive issue to be considered. In the *AT&T* decision cited above, the Court reaffirms that this is the issue for assessing the “useful, concrete, and tangible” nature of a set of claims under 101 doctrine. Accordingly, Examiner views the *Warmerdam* holding as the dispositive issue in this analogous case.

14. The fact that the invention is merely the manipulation of *abstract ideas* is clear. The data referred to by Applicant’s phrases “information identifying … users that are members of the group” and “information identifying … items that are members of the group” are simply abstract constructs that do not limit the claims to the transformation of real world data (such as monetary data or heart rhythm data) by some disclosed process. Consequently, the necessary conclusion under *AT&T*, *State Street* and *Warmerdam*, is straightforward and clear. The claims take several abstract ideas (i.e., “information identifying … users that are members of the group” and “information identifying … items that are members of the group” in the abstract) and manipulate them together adding nothing to the basic equation. Claims 1-80 are, thereby, rejected under 35 U.S.C. 101.

15. Regarding the “system” recitals in claims 59-65, and 77-80 and the presumed “product of manufacture” claims in claims 67-76, the invention is still found to be nonstatutory. Any other finding would be at variance with current case law. Specifically, the Federal Circuit held in *AT&T v. Excel*, 50 USPQ2d 1447 (Fed. Cir. 1999) that:

Art Unit: 2121

Whether stated implicitly or explicitly, we consider the scope of Section 101 to be the same regardless of the form -- machine or process -- in which a particular claim is drafted. AT&T v. Excel, 50 USPQ2d 1447, 1452 citing In re Alappat, 33 F.3d at 1581, 31 USPQ2d at 1589 (Rader, J., concurring) (emphasis added.)

16. Examiner considers the scope of Section 101 to be the same regardless of whether Applicant *claims* a “process”, “machine”, or “product of manufacture”. While the “system” recitals in the preambles of claims 59-65, and 77-80 make the claims ostensibly drawn to be “apparatus” claims, they are insufficient by themselves to limit the claims to statutory subject matter. Likewise, the presumed attempts to limit claims 67-76 to “product of manufacture” claims are insufficient by themselves to limit the claims to statutory subject matter. Examiner’s position is clearly consistent with *Alappat*, and *AT&T* and is implicitly consistent with *Warmerdam* and *State Street*. Accordingly, those claims are also properly rejected.

Claim Rejections - 35 U.S.C. § 112

The following is a quotation of the first paragraph of 35 U.S.C. §112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-80 are rejected under 35 U.S.C. §112, first paragraph because current case law (and accordingly, the MPEP) require such a rejection if a §101 rejection is given because when Applicant has not in fact disclosed the practical application for the

Art Unit: 2121

invention, as a matter of law there is no way Applicant could have disclosed *how to* practice the *undisclosed* practical application. This is how the MPEP puts it:

(“The how to use prong of section 112 **incorporates as a matter of law** the requirement of 35 U.S.C. 101 that the specification disclose as a matter of fact a practical utility for the invention.... If the application fails as a matter of fact to satisfy 35 U.S.C. § 101, then the application also fails as a matter of law to enable one of ordinary skill in the art to use the invention under 35 U.S.C. § 112.”); In re Kirk, 376 F.2d 936, 942, 153 USPQ 48, 53 (CCPA 1967) (“Necessarily, compliance with § 112 requires a description of how to use presently useful inventions, otherwise an applicant would anomalously be required to teach how to use a useless invention.”). See, MPEP 2107.01(IV), quoting In re Kirk (emphasis added).

Therefore, claims 1-80 are rejected on this basis.

Claim Rejections - 35 U.S.C. § 102

17. The following is a quotation of the appropriate paragraphs of 35 U.S.C. §102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

18. Claims 1-2, 7-16, 26-34, 41-42, 44-58, 60-75, and 77-80 are rejected under 35 U.S.C. §102(b) as being anticipated by Brown et al. (U.S. Patent Number 5,557,686; dated 09/17/1996; class 382; subclass 115). Specifically:

Claim 1

Claim 1's "retrieving information identifying, for each of a plurality of groups, users that are members of the group;" is anticipated by Brown et al, col. 2, lin. 3-7, where it recites:

Accordingly, one object of this invention is to provide a method and apparatus for verifying the authenticity of a user of a system having a low imposter pass rate, a low false alarm rate, while only requiring a small number of keystrokes from the user.

Claim 1's "for each group, analyzing properties of the members of the group to identify properties that distinguish users that are members of the group from users that are not members of the group, the analyzed properties relating to interactions with the subject Web site undertaken by users;" is anticipated by Brown et al, col. 2, lin. 22-25, where it recites:

The self-organizing network outputs purified samples of the authorized user which are similar in nature to each other while discarding samples of the user which are not similar.

Claim 1's "to displaying the properties identified as distinguishing members of the selected group from users that are not members of the selected group;" is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of

Art Unit: 2121

method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 1's "receiving user input specifying a name for the selected group; and" is anticipated by Brown et al, claim 3, where it recites:

3. A method for verifying whether a user of a system is authorized using keystroke information according to claim 2, wherein the purifying step uses a self-organizing neural network to group said imposter training signals and said user training signals into clusters having similar keystroke characteristics.

Claim 1's "persistently storing the specified name in a manner that associates the specified name with the selected group, enabling the specified name to be displayed in conjunction with the selected group at a future time." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114 and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

Claim 2

Claim 2's "The method of claim 1, further comprising, for each selected 1 group, displaying with each property identified for the selected group an icon representing the property." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 7

Claim 7's "A method in a computing system for analyzing each of a plurality of groups of items, comprising:

retrieving information identifying, for each of a plurality of groups, items that are members of the group; and" is anticipated by Brown et al, col. 2, lin. 3-7, where it recites:

Accordingly, one object of this invention is to provide a method and apparatus for verifying the authenticity of a user of a system having a low imposter pass rate, a low false alarm rate, while only requiring a small number of keystrokes from the user.

Art Unit: 2121

Claim 7's "for each group, analyzing attributes of the items of the group to identify attributes that distinguish items that are members of the group from items that are not members of the group." is anticipated by Brown et al, col. 2, lin. 22-25, where it recites:

The self-organizing network outputs purified samples of the authorized user which are similar in nature to each other while discarding samples of the user which are not similar.

Claim 8

Claim 8's "The method of claim 7, further comprising, for each group, generating a characterization of the group that incorporates the attributes identified for the group." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 9

Claim 9's "The method of claim 7, further comprising, for at least one selected group, displaying indications of the identified attributes in conjunction 2 with an indication of the identified group." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Art Unit: 2121

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 10

Claim 10's "The method of claim 7, further comprising, for each selected group, displaying with each attribute identified for the selected group an icon representing the attribute." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 11

Claim 11's "receiving user input specifying a name for the distinguished group; and" is anticipated by Brown et al, claim 3, where it recites:

3. A method for verifying whether a user of a system is authorized using keystroke information according to claim 2, wherein the purifying step uses a self-organizing neural network to group said imposter training signals and said user training signals into clusters having similar keystroke characteristics.

Art Unit: 2121

Claim 11's "persistently storing the specified name in a manner that associates the specified name with the distinguished group, enabling the specified name to be displayed in conjunction with the distinguished group at a future time." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114 and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

Claim 12

Claim 12's "The method of claim 7 wherein the analyzed attributes of the items are binary attributes having one of two possible values." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114 and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing

Art Unit: 2121

the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

Claim 13

Claim 13's "The method of claim 12, further comprising converting values of a multivalued attribute having one of more than two possible values to binary values of an analyzed binary attribute." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114 and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

Claim 14

Claim 14's "The method of claim 12, further comprising converting values of a continuous attribute having any of a range of numerical values to binary values of an analyzed binary attribute." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114 and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that

Art Unit: 2121

host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

Claim 15

Claim 15's "The method of claim 7 wherein the analyzed attributes of the items are multivalued attributes having one of more than two possible values." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114 and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

Claim 16

Claim 16's "The method of claim 7 wherein the analyzed attributes of the items are continuous attributes having any of a range of numerical values." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114

Art Unit: 2121

and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

Claim 26

Claim 26's "A computer-readable medium whose contents cause a computing system to analyze each of a plurality of groups of items by: retrieving information identifying, for each of a plurality of groups, items that are members of the group; and" is anticipated by Brown et al, col. 2, lin. 3-7, where it recites:

Accordingly, one object of this invention is to provide a method and apparatus for verifying the authenticity of a user of a system having a low imposter pass rate, a low false alarm rate, while only requiring a small number of keystrokes from the user.

Claim 26's "for each group, analyzing attributes of the items of the group to identify attributes that distinguish items that are members of the group from items that are not members of the group." is anticipated by Brown et al, col. 2, lin. 22-25, where it recites:

The self-organizing network outputs purified samples of the authorized user which are similar in nature to each other while discarding samples of the user which are not similar.

Claim 27

Claim 27's "The computer-readable medium of claim 26 wherein the contents of the computer-readable medium further cause the computing system to, for each group, generate a characterization of the group that incorporates the attributes identified for the group." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 28

Claim 28's "The computer-readable medium of claim 26 wherein the contents of the computer-readable medium further cause the computing system to, for at least one selected group, display indications of the identified attributes in conjunction with an indication of the identified group." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Art Unit: 2121

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 29

Claim 29's "displaying information identifying the selected group; and" is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 29's "in conjunction with the displayed information identifying the selected group, displaying one or more icons, each icon indicating a characteristic of members of the selected group that differentiates typical members of the selected group from typical members of the other groups." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of

method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 30

Claim 30's "The method of claim 29 wherein a plurality of icons are displayed, and wherein the plurality of icons is displayed in an order corresponding to the extent to which the characteristic indicated by each differentiates typical members of the selected group from typical members of the other groups." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 31

Claim 31's "The method of claim 29, further comprising displaying, in conjunction with each displayed icon, an indication of the extent to which the characteristic indicated

Art Unit: 2121

by each differentiates typical members of the selected group from typical members of the other groups." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 32

Claim 32's "The method of claim 29, further comprising displaying, in conjunction with each displayed icon, a shape whose length indicates the extent to which the characteristic indicated by the displayed icon differentiates typical members of the selected group from typical members of the other groups." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 33

Claim 33's "The method of claim 29, further comprising displaying, in conjunction with each displayed icon, an indication of the extent to which the members of the selected group has the characteristic indicated by the icon." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 34

Claim 34's "The method of claim 29, further comprising displaying, in conjunction with each displayed icon, the percentage of the members of the selected group has the characteristic indicated by the icon." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Art Unit: 2121

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 41

Claim 41's "The method of claim 29 wherein the characteristic indicated by a distinguished one of the displayed icons is possession of a distinguished attribute by at least a portion of the members of the selected group." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 42

Art Unit: 2121

Claim 42's "The method of claim 29 wherein the characteristic indicated by a distinguished one of the displayed icons is non-possession of a distinguished attribute by at least a portion of the members of the selected group." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 44

Claim 44's "The method of claim 29 wherein one of the displayed icons conveys the likeness of a shopping basket." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 45

Claim 45's "The method of claim 29 wherein the displayed icons are brand logo icons that indicate actions related to one or more brands of products." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 46

Claim 46's "The method of claim 29 wherein one of the displayed icons conveys the likeness of a shopping basket overlaid by a circle-slash symbol indicating negation." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of

Art Unit: 2121

method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 47

Claim 47's "The method of claim 29 wherein one of the displayed icons indicates a high number of item purchases." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 48

Claim 48's "The method of claim 29 wherein one of the displayed icons indicates a low number of item purchases." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Art Unit: 2121

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 49

Claim 49's "The method of claim 29 wherein one of the displayed icons conveys the likeness of a coupon." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 50

Claim 50's "The method of claim 29 wherein one of the displayed icons conveys the likeness of a coupon overlaid by a circle-slash symbol indicating negation." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 51

Claim 51's "The method of claim 29 wherein one of the displayed icons indicates a high level of coupon use." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 52

Claim 52's "The method of claim 29 wherein one of the displayed icons indicates a low level of coupon use." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 53

Claim 53's "The method of claim 29 wherein one of the displayed icons conveys the likeness of a dollar sign." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has

Art Unit: 2121

not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 54

Claim 54's "The method of claim 29 wherein one of the displayed icons conveys the likeness of a dollar sign overlaid by a circle-slash symbol indicating negation." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 55

Claim 55's "The method of claim 29 wherein one of the displayed icons indicates a high level of spending." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 56

Claim 56's "The method of claim 29 wherein one of the displayed icons indicates a low level of spending." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 57

Claim 57's "The method of claim 29, further comprising displaying a control usable by a user to specify a name for the selected group." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 58

Claim 58's "The method of claim 29 wherein the selected group and the other groups are mutually exclusive, in that no item belongs to more than one group.

Claim 60

Claim 60's "The computing system of claim 59 wherein the display generation subsystem causes a plurality of icons to be displayed, in an order corresponding to the extent to which the characteristic indicated by each differentiates typical members of the selected group from typical members of the other groups." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 61

Claim 61's "The computing system of claim 59 wherein the display generation subsystem causes to be displayed, in conjunction with each displayed icon, an indication of the extent to which the characteristic indicated by each differentiates typical members of the selected group from typical members of the other groups." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 62

Claim 62's "The computing system of claim 59 wherein the display generation subsystem causes to be displayed, in conjunction with each displayed icon, a shape whose length indicates the extent to which the characteristic indicated by the displayed icon differentiates typical members of the selected group from typical members of the other groups." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 63

Claim 63's "The computing system of claim 59 wherein the display generation subsystem causes to be displayed, in conjunction with each displayed icon, the percentage of the members of the selected group has the characteristic indicated by the icon." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has

not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 64

Claim 64's "One or more computer memories collectively containing a data structure identifying possible characterizations of groups of items, comprising a plurality of indications each indicating one of a plurality of possible characterizations of groups of items, such that the contents of the data structure may be used to select possible characterization that characterize a group of items." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 65

Claim 65's "The computer memories of claim 64 wherein the data structure further comprises, for each indicated possible characterization, information identifying an icon associated with the possible characterization, such that the contents of the data

Art Unit: 2121

structure may be used to display icons associated with the selected possible characterizations." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 66

Claim 66's "The computer memories of claim 64 wherein the data structure further comprises, for each indicated possible characterization, information indicating a differentiation threshold, the differentiation threshold indicating the extent to which the subject of the possible characterization must differentiate a group of items from items in other groups in order for the possible characterization to apply to the group of items, such that possible characterizations may be selected based upon satisfaction of their differentiation thresholds." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 67

Claim 67's "One or more generated data signals collectively conveying a data structure indicating a characterization of a group of items, comprising information identifying one or more characteristics that distinguish typical items in the group of items from typical items outside the group of items, such that the contents of the data structure may be used to display characteristics of the group of items that characterize the group of items." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 68

Claim 68's "The generated data signals of claim 67 wherein the data structure is displayable document." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 69

Claim 69's "The generated data signals of claim 67 wherein the data structure is an HTML document." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114 and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

The prior art disclosure does not limit itself to a specific data structure type.

Claim 70

Claim 70's "The generated data signals of claim 67 wherein the data structure is an ActiveX control." is anticipated by Brown et al, col. 6, lin. 5-22, where it recites:

To construct a vector representing the timing of keystroke characteristics, the terminal 100 has clock 104 connected to processor 102 so that the timing of the keystrokes can be determined. The terminal 100 also contains components such as host interface 106 for connecting the terminal to the host, a RAM 108, a ROM 110, a system bus 112, a keyboard interface 114

Art Unit: 2121

and an optional monitor interface 116 connected to optional monitor 118, for example. Processor 102 and clock 104 are used to construct the vector representing the keystroke characteristics of the user. The vector representing the keystroke characteristics can be sent to host 112 so that host 112 can determine whether the user is an authorized user or an imposter. Alternatively, terminal 100 might contain the program used to determine whether the user is authorized or an imposter. The present invention has been successfully tested using a data capture program utilizing the X window system running on an IBM.RTM. R/S 6000 graphics workstation.

The prior art disclosure does not limit itself to a specific data structure type.

Claim 71

Claim 71's "The generated data signals of claim 67 wherein the data structure contains an application that displays characteristics of the group of items in a display area." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 72

Claim 72's "The generated data signals of claim 67 wherein the data structure further comprises, for each identified characteristic, information identifying an icon representing the characteristic, such that the contents of the data structure may be used to display an icon representing each identified characteristic." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 73

Claim 73's "The generated data signals of claim 67 wherein the data structure further comprises information identifying an order for the identified characteristics that reflects the relative extents to which the identified characteristics distinguish typical items in the group of items from typical items outside the group of items, such that the contents of the data structure may be used to display indications of the identified characteristics in the identified order." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 74

Claim 74's "The generated data signals of claim 73 wherein the identified order for the identified characteristics reflects the relative extents to which the identified characteristics distinguish typical items in the group of items from typical items outside the group of items." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Levels of access are depicted by a listing of user/impostor determinations.

Claim 75

Art Unit: 2121

Claim 75's "The generated data signals of claim 67 wherein the data structure further comprises information indicating the extent to which the items in the group of items possess each of the identified characteristics." is anticipated by Brown et al, claim 6, where it recites:

6. A method for verifying whether a user of a system is authorized using keystroke information according to claim 1, wherein the determining step uses a distance method to determine a distance between a vector representative of the signal to be tested and a vector representative of at least one user training signal and if said determined distance is less than a predetermined distance, allowing access to the system.

Claim 77

Claim 77's "One or computer memories collectively containing a data structure indicating a characterization of a group of items, comprising information identifying one or more characteristics that distinguish typical items in the group of items from typical items outside the group of items, such that the contents of the data structure may be used to display characteristics of the group of items that characterize the group of items." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Claim 78

Claim 78's "The computer memories of claim 77 wherein the data structure further comprises, for each identified characteristic, information identifying an icon representing the characteristic, such that the contents of the data structure may be used to display an icon representing each identified characteristic." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 79

Claim 79's "The computer memories of claim 77 wherein the data structure further comprises information identifying an order for the identified characteristics that reflects the relative extents to which the identified characteristics distinguish typical items in the group of items from typical items outside the group of items, such that the contents of the data structure may be used to display indications of the identified characteristics in the identified order." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Displaying the stored data is well within the broadest reasonable interpretation of this disclosure.

Claim 80

Claim 80's "The computer memories of claim 79 wherein the identified order for the identified characteristics reflects the relative extents to which the identified characteristics distinguish typical items in the group of items from typical items outside the group of items." is anticipated by Brown et al, col. 13, lin. 48-59, where it recites:

Alternatively, instead of denying the user access to the system, it is possible to perform other steps. For example, if the user is determined to be an imposter, the user might be required to enter additional password type information. Alternatively, a system operator can be notified that a user has not passed the keystroke test and the system operator might verify that the person at the terminal is actually the authorized user by some other type of method. However, the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter but is applicable to any type of response to the authorized user/impostor determination.

Levels of access are depicted by a listing of user/impostor determinations.

Response to Amendment

Art Unit: 2121

Applicant did not amend his claims to respond to the rejections by Examiner and instead presents arguments as to his theories why the rejections are not accurate.

Examiner disagrees:

Rejections under 35 U.S.C. §101

Applicant argues that the following examples are useful, concrete, and tangible applications:

In at least one embodiment of Applicants' invention, "a software facility ('the facility') [provides] for automatically characterizing and enabling a user to persistently name data segments containing items."

This abstract feature is inherent to standard software languages. The ability to name a simple array of data is an example of this (i.e., `ArrayName[1]`, `ArrayName[2]`, `ArrayName[3]`, ... `ArrayName[N]`.) This is not concrete and tangible. It is well settled that computer programs per se are not statutory. Likewise, elements for constructing computer programs are not statutory either.

The facility "receives information identifying one or more groups of items, such as groups identified among the items using data mining data segmentation techniques," and the information received by the facility "also indicates, for each item in each group which attributes characterize the item from any number of possible attributes (for that item)." (page 4, lines 10-19).

Which attributes? Mathematical attributes? Logical attributes? Physical attributes? Applicant's reference here is broader in practical application (and more abstract) than a pure mathematical algorithm...in fact pure mathematical attributes are a

subset of what Applicant recites here. The concept is not applied to anything. It is just a method for naming groups of abstract things. At least in *In re Warmerdam*, those applicants described a "bubble hierarchy" for their data. In this case, Applicant doesn't even go that far to limit exactly what things are to be named. Applicant's example is again so abstract that a reasonable person looking at the disclosure cannot identify exactly what the naming algorithm is to be applied. It is simply a naming process.

"Based upon the membership of the groups and the attributes of the items in each group, the facility applies additional data mining techniques to identify, for each group, characteristics of the items of the group that most significantly distinguish the group from other groups." (page 4, line 28 to page 5, line 2).

Again, what characteristics? What kind of data is being data mined? Applicant refuses to provide an answer. These questions are critical to determine whether a statutory practical application has been disclosed. Applicant simply recites an abstract description of an algorithm that divides "things" into classes and subclasses. It is not limited to a practical application in the least.

The information presented by the facility gives a user of the facility a sense of the significance of the group it characterizes and enables the user of the facility to compose a mnemonic name for the group (page 5, lines 25-28) and assists the user to conceptualize the significance of a particular group of items and to persistently name the group for future reference. (page 6, lines 3-5).

Again, this description encompasses a simple array or "Typedef" structure in C++. Giving a user a "sense of the significance of the group" is clearly not

Art Unit: 2121

patentable...a sense of significance is simply human thought per se and unpatentable in any form. An abstract facility to compose mnemonic names for data structures encompasses the naming conventions for arrays and "Typedef" structures (e.g., Array1[1], Array1[2], ...Array1[N].) This still does not disclose the thing to which it is applied. It is simply an element of a programming language. As stated before, software programs per se are not patentable. Likewise, abstract elements of such programs are not patentable either.

Aside from the fact that Applicants' evidence for their argument is actually disclosed only in the Specification and is not claimed (and cannot be "read into" the claims under In re Donaldson) Examiner notes that Applicants have not shifted their burden by distinguishing this case from the facts in the case In re Warmerdam, which was the basis of Examiner's rejections in the previous non-final rejection. Claims that are not distinguishable in statutory nature from those in Warmerdam are clearly not statutory so the rejections under 35 U.S.C. §101 STAND.

Rejections under 35 U.S.C. §112, first paragraph

Since the §101 rejections properly stand, the related §112, first paragraph rejections stand as well.,

Rejections under 35 U.S.C. §102

On a preliminary note, Applicant argues that Examiner "dissected" the claims into discrete elements in order to examine them. Examiner disagrees with this argument.

Examiner found the prior art that anticipates Applicants' invention in its entirety...not piecemeal. If it were the case that piecemeal examination was necessary, Examiner would have used a 103 rejection instead of a 102. Examiner does not find that a 103 rejection is appropriate in this case. The invention in its entirety is anticipated by the prior art presented by Examiner.

Examiner discussed each clause written by Applicant in the order presented by Applicant. Examiner highlighted portions of those claims that were especially important, but did not remove portions of the claims in order to examine them... Again, if that were necessary, a 103 rejection would have been used. The entirety of the claims and clauses are anticipated by the prior art selected by Examiner...as will be shown below.

First, applicants argue the following about claim 1:

The cited reference fails to disclose, suggest or teach the step of "**retrieving information** identifying, for each of a plurality of groups, users that are members of the group."

Examiner found that this clause of the claim is anticipated by Brown et al, col. 2, lin. 3-7, where it recites:

Accordingly, one object of this invention is to provide a method and apparatus for verifying the authenticity of a user of a system having a low imposter pass rate, a low false alarm rate, while only requiring a small number of keystrokes from the user.

Applicants' clause discloses that their claimed system "retrieves information". The prior art does the same by capturing the keystrokes of a user, while he uses the computer, in order to analyze the keystroke patterns in order to determine if the user is

an "imposter" or an "authorized user". The two main "groups" the prior art discloses are "imposters" and "authorized users".

The main difference between the claimed invention and the prior art is that the prior art actually discloses the practical application of analyzing keystrokes. In the current application, the claimed invention encompasses this use as well as many other uses because no limitation to a practical application is specified in the claim...it simply retrieves "information identifying, for each of a plurality of groups, users that are members of the group". This could apply to keystroke data, heart rhythm data, facial recognition data, voice data, retinal scan data, fingerprint data, badge number, etc. All of these things operate differently and there is no disclosure in the claim of how to practice the individual applications (hence the 112 rejection.) In fact, there is no limitation to any such practical application at all...hence the 101 rejection. It is clear that the prior art is actually a subset of the unlimited, abstract claim submitted by Applicant.

Applicant further argues that:

...the processed information is associated solely with the user (e.g., the user provided the information). Moreover, the same user may provide information that is different from information previously provided at a prior time. In contrast, in Applicants' invention, the information identifies users that are members of a group, which can be more than one user. Thus, for at least this reason, "verifying the authenticity of a user of a system" is distinct from and not the same as "retrieving information identifying . . . users that are members of the group."

On a threshold issue, much of what Applicant discusses here is not in the claim. Furthermore, the claim is not written in means-plus-function format, so limitations in the Specification cannot be "read into" the claim under In re Donaldson. The claim stands or falls on its own..."in light" of the Specification.

The group in the prior art denoted by "authorized user" is capable of containing more than one user. Furthermore, the group in the prior art denoted by "impostor" may also contain more than one unauthorized user.

Applicant's claim assertion that "...the information identifies users that are members of a group, which can be more than one user" is of no novelty. There is no patentable difference between that and the prior art. In fact, the prior art expressly states that there may be multiple users classified as "authorized" to access a single system. Specifically, in the last sentence of the "Field of the Invention" section recites:

The present invention is applicable to any type of system in which access to the **system** is desired to be limited to authorized users. (Emphasis added.)

Applicant further argues that:

The cited reference fails to disclose, suggest or teach the second feature for at least the reason that the purified samples of a single user (i.e., the authorized user) are distinct from and not the same as the properties of the members of the group. The purified samples are associated with one user (the authorized user) while the properties are associated with the members of the group. Moreover, the Examiner completely failed to consider the latter portion of the second feature, which states "the analyzed properties relating to interactions with the subject Web site undertaken by the users."

It is clear in the abstract of the prior art that the different groups could have multiple users. The prior art states this in the last sentence of the "Field of the Invention" section where it recites:

The present invention is applicable to any type of system in which access to the **system** is desired to be limited to authorized users. (Emphasis added.)

Applicant further argues that:

...the cited reference fails to disclose, suggest or teach the third feature for at least the reason that a response given once the user is determined to be authorized or an imposter is distinct from and not the same as the displaying of the properties that distinguish members of a group.

Again, the prior art states this in the last sentence of the "Field of the Invention" section where it recites:

The present invention is applicable to any type of system in which access to the system is desired to be limited to authorized users. (Emphasis added.)

Applicant further argues that:

The cited reference fails to disclose, suggest or teach the fourth feature for at least the reason that grouping training signals into clusters having similar keystroke similarities is distinct from and not the same as receiving input specifying a name for the group. Where the user can input the name of the group via a sequence of keystrokes, this is distinctly different from the "keystroke characteristics" as disclosed by Brown et al.

Examiner found that this was anticipated by the part of the prior art that discussed using a self-organizing neural network. Why? A self-organizing network is an unsupervised learning method. By definition, it learns patterns in data without being told what it should look for...the clusters it creates have no labels. In order to use the resulting clusters, the user/trainer must tell the system whether the pattern it detected is in the "authorized user" cluster or whether it is in the "imposter" cluster (The training

Art Unit: 2121

user knows this because he knows which user the training data came from. He knows whether that user is authorized or not.) Labeling a cluster is not novel or non-obvious in the art and the rejection of this claim STANDS.

Applicant further argues that:

The cited reference fails to disclose, suggest or teach the final feature for at least the reason that a terminal containing a program is distinct from and not the same as persistently storing the specified name. Moreover, "enabling the specified name to be displayed in conjunction with the selected group at a future time" as recited by the latter part of the final feature is not and cannot be the same as a terminal containing a program used to authorize a user as disclosed in Brown et al.

This feature is inherent to a classifier system. If the name of the cluster weren't stored, the system wouldn't be able to tell the operational user the result of the classification process. The prior art tells the operational user which users are "authorized" and which are "imposters". In order to tell the operational user the difference, the program needs to know the difference... it needs to have learned the labels from the training user.

Applicant further argues that:

The cited reference fails to disclose, suggest or teach the second feature for at least the reason that outputting purified samples of a single user (i.e., the authorized user) is distinct from and not the same as "analyzing attributes of the items of the group to identify the attributes that distinguish items that are members of the group from items that are not members of the group." Similar to the reasoning provided above in conjunction with Claim 1, the cited reference disclose:, processing of input provided by a at most a single authorized user, which is not the same as analyzing the attributes of the items of the group in that there may be more than one item in the group.

Art Unit: 2121

The "Field of the Invention" section of the prior art expressly makes clear that the different groups could have multiple users. There it recites:

The present invention is applicable to any type of system in which access to the **system** is desired to be limited to authorized users. (Emphasis added.)

Applicant further argues that:

...Examiner seems to have failed to address the last feature of Claim 59. Because the Examiner used the same reference in Brown et al. to reject the other features of Claim 59, Applicants will assume that this same reference will be applied to the last feature of Claim 59.

Examiner did make a mistake with that claim. The last feature was not addressed. Upon additional consideration of that claim, the §102 rejection is withdrawn from that claim only because Applicant, otherwise, would not have sufficient opportunity to comment on any further rejections Examiner would make against that clause of the claim.

Applicant further argues that:

With reference to independent Claims 67 and 77, the Examiner indicated that each of the claims is also anticipated by Brown et al. col. 13, lines 48-59, as recited above. In each rejection, other than again making a specific reference to the portion of the cited reference that states "the invention is not limited to giving a specific response once the user is determined to be authorized or an imposter, but is, applicable to any type of response to the authorized user/impostor determination," the Examiner gave no further statement or indication as to how the language of the claim has been interpreted to support the rejection as required by MPEP 2100. In response, Applicants point out that the cited reference of Brown et al. has to do with a response that is given subsequent to an authorized user/impostor determination. This is distinctly different than and fails to disclose, suggest or teach "information identifying one or more characteristics that distinguish typical items in the group of items from typical items outside the group of items" as recited in each of Claims 67 and 77.

There is no need for Examiner to define the outer bounds of a reasonable interpretation of the prior art. None of those interpretations was claimed. Therefore, those unclaimed interpretations are not legally relevant to the issues relating to the current claims. It is sufficient for Examiner to say that Applicant's current claim is anticipated by the broadest reasonable interpretation of the prior art.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Wilbert L. Starks, Jr. whose telephone number is (703) 305-0027.

Alternatively, inquiries may be directed to the following:

Art Unit: 2121

S. P. E. Anthony Knight (703) 308- 3179

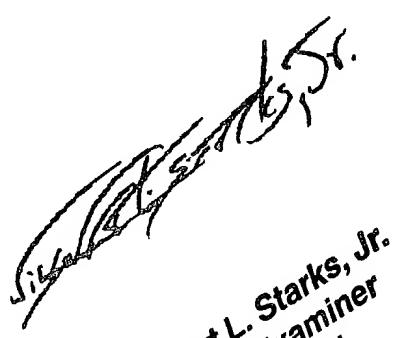
After-final (FAX) (703) 746-7238

Official (FAX) (703) 746-7239

Non-Official/Draft (FAX) (703) 746-7240

WLS

06 August 2004



Wilbert L. Starks, Jr.
Primary Examiner
Art Unit - 2121